REMARKS

Claims 1-3, 5-14, and 16-24 are pending in the above-identified application, and were rejected. With this Amendment, no claims were amended, added, or cancelled. Accordingly, claims 1-3, 5-14, and 16-24 remain at issue.

I. Double Patenting Rejection of Claims

Claims 1-3, 5-14, and 16-24 were provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-40 of co-pending Application No. 09/944,192. Claims 1-3, 5-14, and 16-24 were provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-28 of co-pending Application No. 09/943,893. Claims 1-3, 5-14, and 16-24 were provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-29 of co-pending Application No. 09/943,858. Claims 1-3, 5-14, and 16-24 were provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-30 of co-pending Application No. 09/943,683. Applicants respectfully defer the submittal of a terminal disclaimer until the final scope of the claims is determined.

II. 35 U.S.C. § 102 Anticipation Rejection of Claims

Claims 1-3, 5-14, and 16-24 were rejected under 35 U.S.C. § 102(e) as being anticipated by Dulude, et al. (U.S. Patent No. 6,310,966). Applicants respectfully traverse this rejection.

As discussed in the response to the June 24, 2005 office action, in Dulude et al., the input data are processed with the **private** key 36 of a certifying authority to generate a digital biometric certificate 38, which is sent to the memory for storage and subsequent use to authenticate the first user and associated electronic transactions of the first user. (See col. 4, lines 61-65.) The Examiner cites to column 6, lines 58-65, which states that the public key 70 of the certifying authority is used to **decrypt** the biometric certificate 68 (which was stored as biometric certificate 38 in memory 66) to extract the user public key 74. Thus, in Dulude et al., the private key 36 of a certifying authority is used to encrypt the input data, and the public key 70 of the certifying authority is used to decrypt the biometric certificate. Dulude et al. does not disclose or suggest template information encrypted using a public key of the personal identification certificate authority, as required by claim 1.

Moreover, in Dulude, et al., the biometric certificate generator 32 of a **registration authority** 34 generates the biometric certificate, whereas the private key 36 of a **certifying authority** is used to encrypt the input data. (See col. 4, lines 55-61.) Thus, Dulude, et al. does not disclose or suggest that the person identification certificate is generated by the personal identification certificate authority, as required by claim 1.

Accordingly, claim 1 is allowable over Dulude, et al. For similar reasons, claims 2-3, and 5-12, which depend from claim 1, and claims 13-14 and 16-24 are also allowable over Dulude et al. Accordingly, Applicants respectfully request withdrawal of this rejection.

III. Conclusion

In view of the above amendments and remarks, Applicants submit that all claims are clearly allowable over the cited prior art, and respectfully request early and favorable notification to that effect.

Respectfully submitted,

Dated: May 15, 2006

By:
Marina N. Saito
Registration No. 42,121
SONNENSCHEIN NATH & ROSENTHAL LLP
P.O. Box 061080
Wacker Drive Station, Sears Tower
Chicago, Illinois 60606-1080
(312) 876-8000